REMARKS

Claims 1, 2, 4-20, 31, 38-41, and 43-48 are pending in the application.

The examiner rejected independent claims 1, 38, and 47 under 35 U.S.C. §103(a) as being unpatentable over Jones in view of ElGamal.

We thank the examiner for the telephonic interview of November 6, 2006, in which claims 1, 38, and 47 were discussed relative to ElGamal. Specifically, the limitation "the server cannot feasibly determine the client secret or the third secret" was discussed. As the Interview Summary dated November 27, 2006 indicates, it was agreed that amending the independent claims to clarify that the server cannot feasibly determine the client secret and cannot feasibly determine the third secret would overcome the ElGamal rejection.

Accordingly, we have amended independent claims 1, 38, and 47 to recite that "the server cannot feasibly determine the client secret and cannot feasibly determine the third secret." Support for the amendment can be found at least at [0038]. We submit that the amendment does not change the intended scope of the claims, but rather avoids an unintended interpretation of the previous claim language.

Neither Jones nor ElGamal discloses or suggests a protocol in which "the server cannot feasibly determine the client secret and cannot feasibly determine the third secret," as is recited in claims 1, 38, and 47 as amended. The examiner admits that Jones does not disclose protocols in which "the server cannot feasibly determine the client secret or the third secret," as the claims previously recited, which presumably would also apply to the claims as currently amended. The examiner supplies ElGamal as supposedly disclosing that which is missing from Jones.

However, ElGamal also does not teach or suggest a protocol in which "the server cannot feasibly determine the client secret and cannot feasibly determine the third secret," as is recited in claims 1, 38, and 47 as amended. Instead, ElGamal discloses a protocol in which party A and party B, which the examiner equates with the client and server of the claims, have respective secrets x_A and x_B, which the examiner equates with the client and server secrets of the claims. Parties A and B use their respective secrets to compute a shared secret K_{AB}, which the examiner equates with the third secret of the claims (p. 469). The parties then use K_{AB} to securely

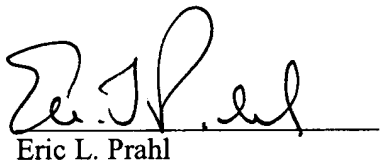
communicate with each other by encrypting their messages. In ElGamal's protocol, parties A and B do not learn the other's respective secret x_A or x_B, but both parties compute and use secret K_{AB}. Thus, if one equates party B with the claimed "server," and K_{AB} with the claimed "third secret," ElGamal explicitly teaches away from a protocol in which the "server cannot feasibly determine the client secret and cannot feasibly determine the third secret," as is required by claims 1, 38, and 47 as amended, and claims dependent thereon.

Therefore, the claims as amended are patentable over Jones in view of ElGamal. None of the other art cited by the examiner supplies that which is missing from Jones and ElGamal.

For at least the reasons stated above, applicant believes the pending application is in condition for allowance, and respectfully requests the examiner allow the claims to issue. No fees are believed to be due at this time. However, please charge any fees, or credit any overpayments, to Deposit Account No. 08-0219.

Respectfully submitted,

Dated: January 24, 2007



Eric L. Prahl
Registration No.: 32,590
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)